JOHN M. NEUKOM (CA Bar No. 275887)
johnneukom@quinnemanuel.com
JORDAN R. JAFFE (CA Bar No. 254886)
jordanjaffe@quinnemanuel.com
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, California 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

DANIEL B. OLMOS (CA Bar No. 235319)
dolmos@nbbolaw.com
NOLAN, BARTON, BRADFORD, OLMOS LLP
600 University Avenue
Palo Alto, CA 94301
Telephone: (650) 326-2980
Facsimile: (650) 326-9704

Attorneys for Plaintiff FORTINET, INC.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FORTINET, INC., a corporation

Plaintiff,

vs.

SOPHOS, INC., a corporation, MICHAEL VALENTINE, an individual, and JASON CLARK, an individual.

Defendants.

SOPHOS INC. and SOPHOS LTD., corporations,

Counterclaim Plaintiffs,

vs.

FORTINET, INC., a corporation,

Counterclaim Defendant.

Case No. 3:13-cv-05831-EMC (DMR)

FORTINET, INC.'S REPLY IN SUPPORT OF MOTION FOR SANCTIONS PURSUANT TO FED. R. CIV. P. 37 AND 28 U.S.C. § 1927

Judge: Honorable Donna M. Ryu
Date: August 27, 2015
Time: 11:00 AM

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes and Rules

Other Authorities

I. LIMITED SANCTIONS ARE APPROPRIATE UNDER 28 U.S.C. § 1927

Fortinet requests limited sanctions under 28 U.S.C. § 1927, and the Court's inherent authority, in the form of a small portion of the attorney's fees and costs that Fortinet incurred starting in May 2015. Fortinet requests (i) $84,768.74 in known fees and costs, Neukom Decl. (submitted with initial Motion) at ¶ 46, and (ii) reasonable fees and costs in an amount to be determined based on Fortinet's litigation of the instant motion. In opposing Fortinet's motion, Sophos has not objected to the reasonableness of the amounts of those fees and costs. *See generally* Opp. (not objecting on these bases). Fortinet incurred those fees and costs during a period of less than two months, between early May 2015 and late June 2015, and directly in response to Sophos' opposition to Fortinet's requested discovery (since granted) and two motions to compel.

At issue in the instant motion is whether Fortinet should have to shoulder those fees and costs. Fortinet asks for recovery of its attorney's fees and expenses on the specific bases that Sophos' counsel—in May and June 2015—made a series of knowing misrepresentations, relied on them to withhold discovery, and furthermore asked this Court to rely on them to deny Fortinet's motions to compel. *See* Mot. at 21-22 (identifying in "bullet point" format eight specific bases for sanctions under § 1927, most of which are demonstrable misstatements of fact or law).

A. Factual Misrepresentation: Sophos Counsel Produced "All Potentially Relevant" Documents from the Sophos-Issued Laptops by May 2015

On June 2, 2015, Fortinet filed its second motion to compel (through the Court's joint-letter process) on the subject matter underlying the instant motion for sanctions. Specifically, in that motion to compel, Fortinet asked for "an order compelling Sophos . . . to provide discovery responsive to Fortinet's First Set of Requests for Inspection (Nos. 1-5)." Dkt. No. 138 at 1. Those Requests for Inspection, in turn, asked for inspections and forensic "scans" of various personal and Sophos-issued computer devices used by about ten individuals who previously worked at Fortinet, subsequently joined Sophos, and through whose computing activity (Fortinet alleges)

trade secrets flowed from Fortinet to Sophos. Ex. G (all citations to exhibit numbers, unless otherwise noted, refer to the original motion); *see also* Dkt. No. 9 at ¶ 71-92.

In opposing that motion to compel, Sophos argued that this Court should deny Fortinet's requests for inspections and forensic-scan data because there was no need. There was no need, Sophos counsel argued, because ***all potentially-relevant documents*** from the disputed computer devices had ***already*** been produced earlier in the case. Sophos was crystal clear on this point. Indeed, this was Sophos' lead argument. Dkt. No. 138 at 5 (starting the "Sophos Statement" as follows: "Fortinet's demand to inspect computers owned by its competitor, Sophos, is unwarranted and premature. ***Sophos has recently produced all documents from the Sophos computers that are potentially responsive to Fortinet's document requests related to its claim against Sophos for trade secret misappropriation.***") (emphasis added).

On the next page, Sophos repeated the same factual representation: "Fortinet's inspection request for all Sophos-owned laptops is unwarranted and premature, because ***Sophos has produced all potentially relevant documents from those computers, including for Messrs. Valentine and Clark.***" *Id*. at 6 (emphasis added).

In a footnote on the same page, Sophos repeated a variation of the same factual representation. *Id.* at 6 n.3 ("***On May 29, 2015 . . . Sophos reviewed and produced all previously-withheld potentially relevant documents, Bates numbered 5831_Sophos_00590898 – 00593110.***") (emphasis added).

Months later, it is now clear that those statements were untrue. On June 30, 2015, the Court entered an Order entitling Fortinet (through an e-discovery vendor) to collect and review forensic scan data for the "Sophos-issued" laptops used by former Fortinet employees after they joined Sophos. Dkt. No. 170. These are the exact same Sophos-issued laptops that Sophos refused to produce for inspection for months, refused to produce for inspection in the face of a motion to compel, and from which (in opposing that motion to compel) Sophos represented to the Court it had already produced all potentially relevant documents. Dkt. No. 138 at 5 ("Sophos has recently produced ***all documents*** from the Sophos computers that are ***potentially responsive***")

(emphasis added); *id.* at 6 ("Sophos has produced ***all potentially relevant documents from those computers***") (emphasis added).

In truth, it is now clear, these Sophos-issued laptops are awash in hundreds of thousands of documents that were not produced and that are (to put it mildly) "potentially relevant" to Fortinet's trade-secret claim. Subsequent to the Court's Order, Fortinet obtained 10,681 gigabytes in forensic images of the former Fortinet employees' devices. Dkt. No. 176 at 1-2. Inspection of these images revealed over 1.6 million files/hits containing the term "Fortinet," with 264,124 files/hits on ***Sophos-issued computers*** containing the terms "Fortinet" and "Confidential" and 170,948 files/hits containing the terms "Fortinet" and "Confidential" that appear to have been accessed after the Sophos' employment date of the former Fortinet employee who possessed the file. Mot. at 19-20. Out of the eleven former Fortinet employees that Fortinet obtained devices for, ***all eleven*** had files that contained "Fortinet" and "Confidential" and were accessed after their start date at Sophos. Dkt. No. 176 at 2.

Sophos produced approximately 800,000 documents on Monday, August 3, 2015. Margeson Decl. ¶ 4. Given the massive amount of data, Fortinet is just now able to review it in a searchable database, which—as of Friday, August 7—was still being loaded with Sophos' Monday production. *Id.* A search for "Fortinet" and "Confidential," excluding instances of "Sophos" in the full text field, returned over 30,000 responsive documents. *Id*. Such documents include, *inter alia*, Fortinet's confidential "LeaderBoard" reports, Fortinet internal competitive analyses, highly confidential "Point of Sale" reports, sensitive financial information, and sales presentations labeled "Fortinet Confidential." *Id.* In addition, Sophos produced email chains indicating that a former Fortinet employee would rely on knowledge and contacts developed at Fortinet for Sophos' benefit. *See* Exs. HH & Ex. II.

In its Opposition brief, Sophos dedicates one paragraph to this issue and attempts to soften its prior misstatements. Opp. at 17 (arguing that Sophos "intended" to represent to this Court that it had produced only a sub-set of documents, namely only those that "Sophos's counsel had previously identified" and "did not refer to documents that Sophos's counsel had not yet

reviewed"). But the contents of that paragraph in Sophos' Opposition brief are contradicted by the prior statements of Sophos counsel. For the disputed Sophos-issued laptops, Sophos did not represent that it had produced only a limited sub-set of "potentially relevant" documents, nor admit that the devices contained any "potentially relevant" documents that Sophos counsel had not yet reviewed or produced. Instead, Sophos counsel repeatedly told Fortinet and this Court in unqualified language that "Sophos has recently produced all documents from the Sophos computers that are potentially responsive to Fortinet's document requests related to its claim against Sophos for trade secret misappropriation" and that "Sophos has produced all potentially relevant documents from those [Sophos-issued] computers, including for Messrs. Valentine and Clark." Dkt. No. 138 at 5-6. As Fortinet know nows, those statements were wrong to the tune of multiple hundreds of thousands of (withheld) documents.

Finally, what makes these factual misrepresentations especially difficult to swallow is the timing. It is now clear that Sophos counsel and its e-discovery vendor collected forensic scans or "image" files of the disputed Sophos-issued laptops in May 2014. *See* Read Decl. at ¶ 4 (declaring that the acquisition logs and/or the "dates" for the forensic image files that Sophos was recently ordered to produce show that Sophos imaged the Sophos-issued laptops for ten of the eleven former Fortinet employees in May 2014, and the eleventh in August 2014). It is also now clear that those Sophos-issued laptops—even when imaged in May 2014—contained multiple hundreds of thousands of documents that are relevant according to even the most basic search criteria, such as documents that contain the words "Fortinet" and "Confidential" and that contain meta-data showing they were accessed by the former Fortinet employees after they joined Sophos. Dkt. No. 176 at 1-2.

B. <u>Another Factual Misrepresentation</u>: Sophos Lacked "Possession, Custody or Control" of Personal Devices Used by Former Fortinet Employees

In March 2015, Fortinet requested inspections and forensic scanning of various computer devices used by the former Fortinet employees. Ex. G. Those requests covered both personal computers and Sophos-issued computers used by the former Fortinet employees so long as (for

example) those individuals accessed those computers during relevant time periods and/or for purposes of their employment at Fortinet or Sophos. *See id.* at 5.

In response, Sophos counsel produced no such devices for inspection and, instead, served written objections and responses. Ex. H. In numerous places in those written objections and responses, Sophos counsel made conditional objections on the basis that Sophos might lack possession, custody or control of various of the requested devices. Fortinet has not argued that any such conditional objections were factual misrepresentations that should serve as the basis for sanctions. For example, Fortinet has no complaint regarding Sophos' third General Objection covering all requests for various computing devices: "Sophos ***objects*** to these requests ***to the extent*** they seek inspection of items not within the possession, custody or control of Sophos." Ex. H at 1 (emphasis added). Likewise, Fortinet has no complaint regarding the conditional objection made by Sophos counsel in response to each of the five requests for inspection: "***Objection***. . . . This request seeks items that ***may be*** outside of Sophos's possession, custody and control." Id. at 2 (emphasis added).

If Sophos counsel had stopped with those conditional objections, there would be no dispute on this specific issue. But Sophos counsel went further. After lodging conditional objections across all requested devices, Sophos counsel then made an affirmative factual representation in the "response" section for each request, and made that representation specific to the "personal computers" for the former Fortinet employees. "***Sophos responds as follows***: ***To the extent Fortinet is seeking to inspect the Former Fortinet Employee's*** [sic] ***personal computers and devices, those computers and devices are outside of Sophos's possession, custody and control***." Ex. H at 2.

That was not an objection (it was instead a response), and it was not conditional (it was instead an affirmative statement of fact). It was also untrue. Sophos counsel knew its April 2015 statement of fact was untrue because—Fortinet now has forensic evidence to prove—Sophos' litigation counsel (DLA Piper) and its e-discovery vendor (Discovia) collected forensic "image" files of ***personal computers and devices*** of the former Fortinet employees at the outset of this case

in 2014. *See* Read Decl. at ¶ 4 (declaring that the "image" files recently provided to Stroz Friedberg, Fortinet's forensic e-discovery vendor, in response to the Court's order compelling production of those files, include 36 image files; cover dozens of "personal" devices for the former Fortinet employees; and that the "acquisition logs, or the date of the files/folders for each item" show that 34 of these 36 image files were collected by Sophos' counsel and e-discovery vendor from May-September 2014).

Sophos addresses this issue on pages 14-15 of its Opposition Brief but misses the point. Sophos focuses on the "objections" that it lodged and stated in the conditional in response to Fortinet's inspection requests, and observes that such conditional objections are defensible to account for the possibility that some of the requested devices might have (e.g.) disappeared or been disposed of or sold. *See* Opp. at 14 ("Sophos's ***objections*** were warranted because Fortinet's inspection requests encompassed ***many devices*** that are outside of Sophos's possession, custody or control, such as devices used by the former Fortinet employees that are no longer in those employees' possession. *See, e.g.*, Fortinet Ex. H at 1.") (emphasis added). That is beside the point because Sophos counsel did not just lodge conditional objections—and Fortinet has no complaint with the "general objection" cited to by Sophos in the Opposition brief. Fortinet's complaint is that Sophos counsel went a step further and made an affirmative factual representation—not a conditional objection—that Sophos in fact lacked possession or custody or control of ***any*** such "personal" devices of any of the former Fortinet employees. Ex. H at 2. That representation is just plain wrong, and Sophos counsel knew it was wrong. Sophos counsel knew it was wrong because (in reality) Sophos's counsel and e-discovery vendor had taken possession of dozens of these "personal" devices a year earlier in 2014 and created forensic "image" files of them. *See* Read Decl. at ¶ 4.

Sophos also argues that it "repeatedly told Fortinet that Sophos's counsel had imaged the Sophos-issued laptops, but ***only had a few of the employees' personal computers***[.]" Opp. at 15 (emphasis added). That argument has numerous problems. ***First***, it is supported only by Paragraph 9 of the Cunningham Declaration. That paragraph from Mr. Cunningham carefully

avoids making a statement based on personal knowledge ("***I understand that*** . . . "); studiously avoids identifying any speaker ("Sophos's counsel repeatedly told Fortinet that . . . "); and is not supported by a single piece of written correspondence. ***Second***, even if it were true that "Sophos's counsel repeatedly told Fortinet that Sophos's counsel . . . only had a few of the employees' personal computers," even that statement would have been untrue and to the tune of multiple dozens of devices. The evidence now shows that—***since 2014***—Sophos counsel possessed "image" files for 25 personal computing devices used by the former Fortinet employees (seven personal laptops, 15 smart phones such as iPhones, and three tablets). *See* Read Decl. at ¶ 4. ***Third***, the idea that Sophos counsel "came clean" about its actual possession (since 2014) of image files for dozens of the disputed personal devices of the former Fortinet employees is contradicted by Sophos' written correspondence in the final weeks of fact discovery, in which Sophos counsel represented it had collected personal devices from only two employees. *See* below.

C. <u>Another Factual Misrepresentation</u>: By May 27, 2015, Sophos Counsel Had Gathered Personal Devices For Only Krause And Acosta

Not only did Sophos counsel state (untruthfully) on April #, 2015, that Sophos lacked possession, custody or control of any "personal" computing devices for the former Fortinet employees, Sophos counsel then continued the hoax almost two months later. On May 27, Sophos counsel represented that it had personal computing devices for only Kendra Krause and Jason Acosta. Ex. M at 5 ("Sophos confirmed that it currently has devices from Kendra Krause and Jason Acosta . . . "). In truth, Sophos' counsel and e-discovery vendor ***in 2014*** had collected "image" files for 25 personal laptops and smart phones and computer tablets spanning every single former Fortinet employee. Read Decl. at ¶ 4. How can Sophos counsel square its May 27 representation with subsequent evidence that has come to light? *Compare* Ex. M at 5, *with* Read Decl. at ¶ 4.

In its Opposition, Sophos argues that it failed to disclose only its prior possession of Dolph Smith's personal laptop. Opp. at 16-17. But the personal "devices" that Sophos' counsel and e-

discovery had collected (starting a year earlier) and yet failed to disclose on May 27 included dozens of smart phones and tablets that were nowhere mentioned. Indeed, even when Sophos relented some weeks later and permitted Fortinet's e-discovery vendor ten hours to review image files of the "personal" devices of various former Fortinet employees, all such smart phones and tablets were omitted. *Compare* Ex. S at ¶ 8 (listing seven laptop computers made available for an on-site review), *with* Read Decl. at ¶ 4 (listing dozens of smart phones and tablets with "image" files created in 2014).

D. Blatantly Wrong Legal Argument: *Res Judicata*

Sophos opposed Fortinet's first motion to compel on this subject matter—in which Fortinet requested inspections for the devices of former Fortinet employees Michael Valentine and Jason Clark—by making a *res judicata* argument. Sophos argued that (i) Fortinet pleaded claims of trade secret misappropriation against Valentine and Clark in the private arbitration (which is not true); (ii) the arbitrator rejected those claims; and that (iii) Fortinet was therefore barred from seeking any discovery into the computing devices of Valentine and Clark in this case in its pursuit of a statutory trade secret claim against Sophos. Dkt. No. 130 at 5-6. This argument was wrong—and Sophos counsel knew or should have known it was wrong—a few times over.

First, the doctrine of "[r]es judicata, or claim preclusion, bars a party from asserting claims that were, or could have been asserted in an earlier suit ***between the same parties***." *Gonzales v. Wells Fargo Bank NA*, No. C 14-03850 JSW, 2015 WL 877440, at *2 (N.D. Cal. Feb 27, 2015) (emphasis added). The private arbitration included claims against Valentine and Clark (and no statutory claim for trade secret misappropriation) and no claims against Sophos. Exs. A & B. This case includes a statutory claim for trade secret misappropriation against Sophos and no claims against Valentine and Clark. Dkt. No. 9. Given that Sophos was not a party to the private arbitration it cannot—as a matter of law—argue that *res judicata* bars Fortinet from pursuing any claim in this case. By arguing to the contrary in May 2015, Sophos counsel asked this Court to ignore a legal principle that is bedrock.[1] ***Second***, even if *res judicata* applied here (it does not),

[1] The idea that *res judicata* could apply to bar claims between two different legal proceedings in which the parties were ***not*** the same is so absurd that even the most cursory review of

that might bar a legal claim or a factual dispute. But the doctrine does not bar discovery. *See, e.g.*, *Gonzales*, 2015 WL 877440, at *2 .

From May 12, 2015, to the present, Fortinet has been asking Sophos to identify a single legal authority to support its baseless argument that relevant ***discovery*** could be withheld in a different litigation among ***different parties*** under the doctrine of *res judicata*. Ex. K at 1 ("If Sophos is aware of any authority to the contrary, please provide it before our scheduled meet and confer."); Dkt. No. 130 at 4-5 (adducing case law authority for the propositions that *res judicata* does not apply between proceedings with different parties, and even then it cannot be used to bar discovery); Mot. at 22 (challenging the tenability of Sophos' *res judicata* theory). Sophos has yet to respond with a single legal authority to support its position, and that includes its Opposition to the instant motion. Opp. at 17 (arguing *ipse dixit* that "Sophos's *res judicata* argument was and is a correct statement of the law, and Sophos fully intends to pursue that argument at the appropriate time," without providing this Court or Fortinet a single legal authority).

E. Chicanery: Changing Positions, Misleading Statements

Amidst these misstatements of fact and law, it appears that Sophos counsel played a game in efforts to deny and delay any discovery into the computing devices used by the former Fortinet employees. This included misleading positions—such as objecting to forensic scans requested by Fortinet on the basis of "burden" without acknowledging (indeed, while concealing) that Sophos counsel performed 34 forensic scans of the very same devices a year earlier in the case. *Compare* Ex. H at 2-5 (objecting to Fortinet's inspection requests by as "unduly burdensome") and Ex. N at 1 (explaining on June 1, 2015, that Sophos would not produce any Sophos-issued laptops for forensic scans unless Fortinet could justify the "burdensome and intrusive inspection of Sophos's computers"), *with* Read Decl. at ¶ 4 (showing that Sophos' counsel in fact had already collected 34 forensic images of these exact same devices in 2014, and two more in 2015). In the Opposition

---

authorities shows it is dead wrong wrong. Sophos counsel could have discovered its error by checking the case law. *See* above. Or by consulting Black's Law Dictionary (9th Ed.) ("[a]n affirmative defense barring ***the same parties*** from litigating a second lawsuit on the same claim") (emphasis added). Or by referring to a practice guide. *See, e.g.*, Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 4449 (2d ed. 2015) ("The basic premise of preclusion is that parties to a prior action are bound and nonparties are not bound.").

brief, Sophos argues that its burden objections were fair because it "had not scanned all of the devices previously." That is just plain wrong with respect to the Sophos-issued laptops for which Sophos made a "burden" argument as late as June 2015. Read Decl. at ¶ 4 (showing that, of the Sophos-issued laptops, every single one of them was "imaged" by Sophos counsel in May 2014). Sophos also argues that its burden objection was fair because "the burdensome nature of [Fortinet's] request has proved true in the recent weeks." Opp. at 16. That argument misses the point. The point is not that Sophos counsel behaved improperly by objecting to forensic scans as burdensome in any context. The point is that Sophos counsel behaved improperly by making—and repeating into June 2015—"burden" objections to a particular discovery tool (forensic scans) for a collection of computer devices when Sophos counsel itself had already used the exact same tool on the exact same devices in the exact same case. Read Decl. ¶ 4.

Finally, Sophos counsel effectively forced Fortinet to conduct a Fed. R. Civ. P. 30(b)(6) deposition on June 16, 2015, knowing it would be a waste of time, fees and costs. Sophos disputes this in the Opposition. Opp. at 18-19. Fortinet invites the Court to read the historical correspondence to see how this unfolded. Ex. R at 7 (from Fortinet counsel on June 9, asking to schedule the trade-secret deposition after "Sophos complies with the Court's order on Fortinet's motions to compel on its requests for inspection"); *id.* at 6 (from Sophos counsel on June 10: "Sophos will make Mr. Clark available to testify . . . on June 16 . . . If Fortinet elects to forego this deposition at this time, Sophos will not re-designate a witness to testify to those topics"); *id.* at 5 (from Fortinet counsel, later on June 10: "Sophos' position appears to be that despite withholding this [forensic scan] information . . . Fortinet must take Sophos/Mr. Clark's deposition on trade secret issues now or 'forgo' it. As previously explained, Fortient does not believe this is an efficient use of the parties resources given the multiple motions to compel Fortinet has already filed on trade secret issues"); *id.* at 4-5 (from Sophos counsel on June 11, refusing to extend or change the date for the deposition); *id.* at 3-4 (from Fortinet counsel on June 12: "it is most efficient to take Mr. Clark's continued depositions . . . one more time rather than repeatedly. This is most efficient for all involved considering the multiple pending motions to compel. . . . given

Sophos' position that Fortinet must take this deposition now or 'forgo it—a position Fortinet disagrees with—Fortinet will reluctantly take Mr. Clark's deposition on June 16th and then again after Sophos provides the appropriate discovery responsive to Fortinet's requests for inspection").

F. Sophos' Attack on Fortinet's Trade Secret Disclosures Is Both Wrong and Irrelevant

In response to arguments and supporting evidence that Sophos and its counsel behaved improperly on trade secret discovery between May 1, 2015, and late June 2015—and forced Fortinet to litigate two motions to compel until minutes before oral argument—Sophos devotes the plurality of its Opposition brief to arguing that Fortinet's trade secret disclosures during a different time period—between May 2014 and April 2015—were not timely or sufficient. Opp. at 1, 3-8. This argument lacks merit for two reasons. ***First***, it is wrong on the facts. Fortinet repeatedly disclosed trade secrets with particularity—starting in the spring of 2014—and therefore complied with the California Code of Civil Procedure § 2019.210. Indeed, Fortinet put all of those disclosures before the Court in its Motion for Sanctions to remove any question about that. Exs. BB, CC, DD, EE. Fortinet invites the Court to review those disclosures. From the start, they satisfied the California statute. And Sophos' Opposition arguments about why there were deficient are not even supported by the law. For example, Sophos chides Fortinet's early trade secrets disclosures for identifying collections of confidential employee information, such as salaries, as trade secrets. But California law ***supports*** that definition of a trade secret. *See Readylink Healthcare v. Cotton*, 126 Cal. App. 4th 1006, 1018 (2005).

Second, Sophos' argument is irrelevant to the instant motion. Fortinet is not asking for sanctions for Sophos' discovery conduct starting in May 2014 (when Fortinet first served its identification of trade secrets).[2] Instead, Fortinet requests sanctions for the misrepresentations and needless litigation that occurred from May 1, 2015, onward. It is on that date that Sophos admits Fortinet served a trade secrets disclosure sufficient for trade secret discovery to begin. Opp. at 7

[2] If Fortinet were asking for relief for that period of time—during all of which Sophos refused to produce any discovery on trade secrets—the requested sanctions would be many multiples of the amounts currently requested.

("Sophos agreed to accept Fortinet's latest Section 2019.210 disclosure so the parties could complete the remaining discovery . . . ").

G. Sophos' "Inspection Protocol" Argument Is Wrong on the Facts

Sophos also argues that "any delay in [Fortinet's] inspection of the former Fortinet employees' devices after May 11 is on Fortinet, not Sophos" because "Fortinet steadfastly refused to agree to any inspection protocol that did not involve Fortinet's own lawyers at Quinn Emanuel having unfettered access to the data." Opp. at 8.

First, this rationale for withholding evidence is contradicted by the prior writings of Sophos' counsel. From May 1, 2015, onward—into June 2015 and well after May 11, 2015—Sophos counsel made demonstrably untrue representations about the scope of its document productions; relied on factual misrepresentations about what devices were not in its possession; concealed its possession of 34-36 "image" files for over a year for the exact devices being requested; argued implausibly that *res judicata* should bar some of this discovery; and opposed two motions to compel. *See* Mot. at 6-17; above. All of that conduct occurred ***after*** May 11, 2015.

Second, although Sophos insists now that it was willing to produce the requested data all along but-for an acceptable protocol inspection, that is not what the documents show. When Sophos first responded to Fortinet's inspection requests, Sophos did not even mention the issue. Ex. H. Nor did Sophos state that an outside-vendor protocol would be required when it promised it was "revisiting" Fortinet's request to inspect the devices on May 11, 2015. Ex. J. Nor did Sophos limit its arguments against Fortinet's requested discovery, in opposing two motions to compel, to the "protocol" issue by any stretch. Dkt. Nos. 130 (arguing against any discovery whatsoever on *res judicata* grounds) & 138 (arguing against any discovery whatsoever of Sophos-issued laptops).

In fact, lead counsel for Sophos refused Fortinet's requested discovery the ***afternoon before oral argument*** on Fortinet's motions to compel without even a hint at "protocol" concerns. As he described Sophos' position: "***the dispute is about whether Fortinet is entitled to inspect***

images of those employees' Sophos-issued computers or devices. Our position remains that Fortinet is not entitled to that level of access to Sophos-owned property, and nothing in your email below changes our position." Ex. X at 1 (emphasis added). Sophos' lead counsel did not even mention inspection protocol in that email. *See id.*

Third, Sophos' position that Fortinet "refus[ed] for weeks to agree to a reasonable, commonly-used inspection protocol" is simply untrue. *See* Opp. at 10. The historical documents show that (i) Sophos insisted that an outside vendor must be used to review forensic scan data, rather than Quinn Emanuel attorneys in late May, and (ii) Fortinet agreed to that provision on June 9. Ex. P at 4 ("Fortinet intends to inspect the limited machines made available and is working with an outside vendor to allow this under Sophos' improper imposed conditions for inspection.").

II. SOPHOS SHOULD BE SANCTIONED UNDER RULE 37

Fortinet seeks (i) a supplementation of Sophos' "accounting" to remedy the deficiencies and noncompliance with the Court's Order; (ii) production of those devices for inspection; and (iii) attorney's fees for investigating these deficiencies and pursuing the instant motion.

A. Sophos Has Failed to Account for USB Devices and External Devices

The Court's Order required Sophos to "provide an accounting of ***all devices*** in its possession responsive to the Requests, including ***all devices*** currently in Sophos or the Former Fortinet Employees' possession, ***any devices*** that are responsive to the Requests but that no longer exist and/or are now unavailable (including the circumstances why they are unavailable) and identifying any employee for which Sophos contends does not have a ***device*** responsive to the Requests. Sophos will provide this accounting by end of businesses (5:00 PM Pacific) on June 29, 2015." Dkt. No. 170 at 2. The accounting was required to provide information about all devices, including USB devices. Sophos failed to do that.

Sophos is flat wrong that it was required only to attempt to locate the USB devices (but not to account for them). As noted above, the Order clearly requires an accounting of all devices. The Order itself refers to USB devices as "those devices," so Sophos cannot justifiably claim the accounting was not required to include USB devices. Sophos has provided nowhere (including in

the Opposition) an accounting of (i) the USB devices it can identify that could be responsive, and, (ii) whether it could "locate" and/or provide any information regarding where that device is now. This accounting was required by the Court's Order.

B. Sophos Failed to Address All Deficiencies Identified By Fortinet

In addition to the USB devices and external drive discussed above, Fortinet specifically identified Mr. Acosta's work computer, Mr. DeHaven's personal Macbook, Mr. Clark's old personal laptop and current personal computing device, as well as Mr. Archer's personal computer, as devices that were not identified and/or provided to Fortinet as required by the Court's Order. *See* Mot. at 24. Other than a statement that Mr. DeHaven's personal Macbook cannot be obtained by Sophos (if this is indeed what Sophos contends), Sophos fails again to address these deficiencies.

DATED: August 7, 2015

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ John M. Neukom*

John M. Neukom (Bar No. 275887)
johnneukom@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, California 94111-4788
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Plaintiff FORTINET, INC.